A. AMENDMENTS TO CLAIMS

Please cancel Claims 20, 25 and 30 and amend the claims as indicated hereinafter.

1-15. (CANCELED)

16. (CURRENTLY AMENDED) A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message~~ address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm ~~and instructions~~ for decoding the encoded message using the key; and

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message ~~contained in the set of one or more instructions~~ by:

retrieving the ~~key,~~ key from the location specified by the address data and decoding the encoded message using the key.

17. (ORIGINAL) The method as recited in Claim 16, further comprising deleting the retrieved key.

18. (ORIGINAL) The method as recited in Claim 16, wherein the set of one or more instructions comprises a set of Javascript instructions.

19. (ORIGINAL) The method as recited in Claim 16, wherein the set of one or more instructions comprises a set of Java applet instructions.

20. (CANCELED)

21. (CURRENTLY AMENDED) A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message~~ address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm ~~and instructions~~ for decoding the encoded message using the key; and

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message ~~contained in the set of one or more instructions~~ by:

retrieving the ~~key,~~ key from the location specified by the address data and

decoding the encoded message using the key to recover the original message.

22. (ORIGINAL) The computer-readable medium as recited in Claim 21, further carrying one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of deleting the retrieved key.

23. (ORIGINAL) The computer-readable medium as recited in Claim 21, wherein the set of one or more instructions comprises a set of Javascript instructions.

24. (ORIGINAL) The computer-readable medium as recited in Claim 21, wherein the set of one or more instructions comprises a set of Java applet instructions.

25. (CANCELED)

26. (CURRENTLY AMENDED) A computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of::

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message~~ address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm ~~and instructions~~ for decoding the encoded message using the key; and

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message ~~contained in the set of one or more instructions~~ by:

retrieving the ~~key,~~ key from the location specified by the address data and

decoding the encoded message using the key to recover the original message.

27. (ORIGINAL) The computer system as recited in Claim 26, wherein the memory further carries one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of deleting the retrieved key.

28. (ORIGINAL) The computer system as recited in Claim 26, wherein the set of one or more instructions comprises a set of Javascript instructions.

29. (ORIGINAL) The computer system as recited in Claim 26, wherein the set of one or more instructions comprises a set of Java applet instructions.

30. (CANCELED)

31. (CURRENTLY AMENDED) A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key ;

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

32. (ORIGINAL) The method as recited in Claim 31, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further

causes the key to be deleted from the third node after the encoded message is decoded.

33. (CURRENTLY AMENDED) The method as recited in Claim 31, wherein the encoded message and the set of one or more instructions that contain the ~~encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key are contained in ~~comprises~~ an HTML document.

34. (ORIGINAL) The method as recited in Claim 33, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

35. (ORIGINAL) The method as recited in Claim 33, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

36. (ORIGINAL) The method as recited in Claim 35, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

37. (CURRENTLY AMENDED) A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key ;

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

38. (ORIGINAL) The computer-readable medium as recited in Claim 37, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes the key to be deleted from the third node after the encoded message is decoded.

39. (CURRENTLY AMENDED) The computer-readable medium as recited in Claim 37, wherein the encoded message and the set of one or more instructions that contain the ~~encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key are contained in ~~comprises~~ an HTML document.

40. (ORIGINAL) The computer-readable medium as recited in Claim 39, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

41. (ORIGINAL) The computer-readable medium as recited in Claim 39, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

42. (ORIGINAL) The computer-readable medium as recited in Claim 41, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

43. (CURRENTLY AMENDED) A computer system for controlling access to a message that is communicated from a first node to a second node in a network, the computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, causes the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain ~~the encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key;

providing the encoded message and the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

44. (ORIGINAL) The computer system as recited in Claim 43, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes the key to be deleted from the third node after they encoded message is decoded.

45. (CURRENTLY AMENDED) The computer system as recited in Claim 43, wherein the encoded message and the set of one or more instructions that contain the ~~encoded message and~~ instructions for transferring to a third node the encoded message and instructions for retrieving the key are contained in ~~comprises~~ an HTML document.

46. (ORIGINAL) The computer system as recited in Claim 45, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

47. (ORIGINAL) The computer system as recited in Claim 45, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

48. (ORIGINAL) The computer system as recited in Claim 47, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

49-66. (CANCELED)

B. REMARKS

By this amendment, Claims 20, 25 and 30 have been canceled. Hence, Claims 16-19, 21-24, 26-29 and 31-48 are pending in this application. The amendments to the claims do not add any new matter to this application. All issues raised in the Office Action mailed December 12, 2005 are addressed hereinafter.

REJECTION OF CLAIMS 16, 20-22, 25-27, 30-33, 37-39 AND 43-45 UNDER 35 U.S.C. § 102(e)

In the Final Office Action, Claims 16, 20-22, 25-27, 30-33, 37-39 and 43-45 were rejected under 35 U.S.C. § 102(e) as being anticipated by *Matsumoto*, U.S. Patent No. 6,215,877. This rejection is now moot with respect to canceled Claims 20, 25 and 30. It is respectfully submitted that Claims 16, 21, 22, 26, 27, 31-33, 37-39 and 43-45 are patentable over *Matsumoto* for at least the reasons provided hereinafter.

CLAIM 16

Claim 16 is directed to a method for controlling access to a message that is communicated from a first node to a second node in a network. Claim 16, as amended, recites:

> "generating, at the first node, an encoded message by encoding the message with a key;
> generating, at the first node, a set of one or more instructions that contain address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm for decoding the encoded message using the key; and
> providing the encoded message and the set of one or more instructions to the second node;
> wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message by:
> retrieving the key from the location specified by the address data and
> decoding the encoded message using the key."

It is respectfully submitted that Claim 16, as amended, recites one or more limitations that are not taught or suggested by *Matsumoto*. For example, it is respectfully submitted that *Matsumoto* does not teach or suggest at least the Claim 16 limitations "generating, at the first node, a set of one or more instructions that contain address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm for

decoding the encoded message using the key" and "providing the encoded message and the set of one or more instructions to the second node."

In the chat system described in *Matsumoto*, channel secret keys are encrypted and distributed to chat clients in response to a distribution request. The receiving chat clients decrypt the encrypted channel secret keys to recover the channel secret keys. The channel secret keys are maintained at each chat client and are used to encrypt data transmitted onto chat channels and to decrypt data received from chat channels. *Matsumoto* does not teach or suggest that a chat client that generates an encrypted message also generates and sends to the receiving chat client a set of instructions "that contain address data that indicates a location from which the key may be retrieved." This would be unnecessary in the system of *Matsumoto*, since each chat client receives the channel secret keys from the key management server.

Furthermore, *Matsumoto* does not teach or suggest that a chat client that generates an encrypted message also generates and sends to the receiving client a set of instructions "contain ... executable code that implements a decryption algorithm for decoding the encoded message using the key." In the system of *Matsumoto*, each chat client includes an encryption section and a decryption section for encrypting and decrypting chat messages, respectively. There is no indication in *Matsumoto* that chat client receiving a message receives, from the chat client that sent the message, executable code that implements a decryption algorithm.

In view of the foregoing, it is respectfully submitted that at least the Claim 16 limitations "generating, at the first node, a set of one or more instructions that contain address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm for decoding the encoded message using the key" and "providing the encoded message and the set of one or more instructions to the second node" are not taught or suggested by *Matsumoto* and that Claim 16 is therefore patentable over *Matsumoto*.

CLAIMS 21, 22, 26 AND 27

Claim 21 recites limitations similar to Claim 16, except in the context of a computer-readable medium. It is therefore respectfully submitted that Claim 21 is patentable over *Matsumoto* for at least the reasons set forth herein with respect to Claims 16. Claim 22 depends from Claim 21 and includes all of the limitations of Claim 21. Claims 26 and 27 recite limitations similar to Claims 21 and 22, except in the context of apparatuses. It is therefore

respectfully submitted that Claims 26 and 27 are patentable over *Matsumoto* for at least the reasons set forth herein with respect to Claims 21 and 22.

CLAIM 31

Claim 31 is directed to a method for controlling access to a message that is communicated from a first node to a second node in a network. Claim 31, as amended, recites:

> "generating, at the first node, an encoded message by encoding the message with a key;
> generating, at the first node, a set of one or more instructions that contain instructions for transferring to a third node the encoded message and instructions for retrieving the key;
> providing the encoded message and the set of one or more instructions to the second node;
> wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and
> wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:
> the message to be recovered from the encoded message by
> retrieving the key, and
> decoding the encoded message using the key, and
> the recovered message to be provided from the third node to the second node."

According to the approach recited in Claim 31, the originating node (the first node) generates a set of instructions which, when processed by the receiving node (the second node), cause the encrypted message and instructions for retrieving the key to be sent to a third node. The third node decrypts the encrypted message and sends the recovered message back to the second node. Thus, the decrypting of the encrypted message occurs at a different node (the third node) than the node that receives the encrypted message from the sending node (the second node). For example, Claim 31 recites "generating, at the first node, a set of one or more instructions that contain instructions for transferring to a third node the encoded message and instructions for retrieving the key" and "wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node" and "wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes: the message to be recovered from the encoded message by retrieving the key, and decoding the encoded message using the key, and the recovered message to be provided from the third node to the second node."

It is respectfully submitted that these limitations are not in any way taught or suggested by *Matsumoto*. In *Matsumoto*, each chat client decrypts the encrypted messages that it receives using a local copy of the chat channel key that the chat clients received from the key management server. There is no mention or suggestion in *Matsumoto* of a chat client that receives an encrypted message, forwarding the encrypted message to another chat client for decrypting, and then receiving the decrypted message back from that chat client.

The Final Office Action refers to FIGS. 4-7 and the accompanying text of *Matsumoto* for teaching the aforementioned limitations. Applicant has reviewed these portions of *Matsumoto* and cannot find any teaching or suggestion of a chat client receiving an encrypted input signal and forwarding the encrypted input signal to another chat client for decryption in the manner recited in Claim 31. It is therefore respectfully submitted that Claim 31 recites one or more limitations that are not taught or suggested by *Matsumoto* and is therefore patentable over *Matsumoto*.

CLAIMS 32 AND 33

Claims 32 and 33 both depend from Claim 31 and include all of the limitations of Claim 31. It is therefore respectfully submitted that Claims 32 and 33 are patentable over *Matsumoto* for at least the reasons set forth herein with respect to Claim 31. Furthermore, it is respectfully submitted that Claims 32 and 33 recite additional limitations that independently render them patentable over *Matsumoto*.

CLAIMS 37-39

Claims 37-39 recite limitations similar to Claims 31-33, except in the context of computer-readable media. It is therefore respectfully submitted that Claims 37-39 are patentable over *Matsumoto* for at least the reasons set forth herein with respect to Claims 31-33.

CLAIMS 43-45

Claims 43-45 recite limitations similar to Claims 31-33, except in the context of apparatuses. It is therefore respectfully submitted that Claims 43-45 are patentable over *Matsumoto* for at least the reasons set forth herein with respect to Claims 31-33 and 36.

In view of the foregoing, it is respectfully submitted that Claims 16, 21, 22, 26, 27, 31-33, 37-39 and 43-45 are patentable over *Matsumoto*.

REJECTION OF CLAIMS 18, 19, 23, 24, 28, 29, 34-36, 40-42 AND 46-48 UNDER 35 U.S.C. § 103(a)

In the Final Office Action, Claims 18, 19, 23, 24, 28, 29, 34-36, 40-42, and 46-48 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Matsumoto* in view of *Gupta et al.*, U.S. Patent No. 6,226,752 (hereinafter "*Gupta*"). It is respectfully submitted that Claims 18, 19, 23, 24, 28, 29, 34-36, 40-42 and 46-48 are patentable over *Matsumoto* and *Gupta*, considered alone or in combination, for at least the reasons provided hereinafter.

CLAIMS 18 AND 19

Claims 18 and 19 depend from Claim 16 and include all of the limitations of Claim 16. As previously set forth herein, Claim 16 includes one or more limitations that are not taught or suggested by *Matsumoto*. It is also respectfully submitted that these limitations are also not taught or suggested by *Gupta* and *Gupta* was not relied upon in the Final Office Action for teaching these limitations. For example, it is respectfully submitted that at least the limitations "generating, at the first node, a set of one or more instructions that contain address data that indicates a location from which the key may be retrieved and executable code that implements a decryption algorithm for decoding the encoded message using the key" and "providing the encoded message and the set of one or more instructions to the second node" are not taught or suggested by *Gupta*. Accordingly, it is respectfully submitted that Claims 18 and 19 recite one or more limitations that are not taught or suggested by *Matsumoto* or *Gupta*, considered alone or in combination, and are therefore patentable over Claims 18 and 19.

CLAIMS 23 AND 24

Claims 23 and 24 recite limitations similar to Claims 18 and 19, except in the context of computer-readable media. It is therefore respectfully submitted that Claims 23 and 24 are patentable over *Matsumoto* and *Gupta* for at least the reasons set forth herein with respect to Claims 18 and 19.

CLAIMS 28 AND 29

Claims 28 and 29 recite limitations similar to Claims 18 and 19, except in the context of apparatuses. It is therefore respectfully submitted that Claims 28 and 29 are patentable over *Matsumoto* and *Gupta* for at least the reasons set forth herein with respect to Claims 18 and 19.

CLAIMS 34-36

Claims 34-36 depend from Claim 31 and include all of the limitations of Claim 31. As previously set forth herein, Claim 31 includes one or more limitations that are not taught or suggested by *Matsumoto*. It is also respectfully submitted that these limitations are also not taught or suggested by *Gupta* and *Gupta* was not relied upon in the Office Action for teaching these limitations. For example, it is respectfully submitted that at least the limitations "generating, at the first node, a set of one or more instructions that contain instructions for transferring to a third node the encoded message and instructions for retrieving the key" and "wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node" and "wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes: the message to be recovered from the encoded message by retrieving the key, and decoding the encoded message using the key, and the recovered message to be provided from the third node to the second node" are not taught or suggested by *Gupta*. Accordingly, it is respectfully submitted that Claims 34-36 recite one or more limitations that are not taught or suggested by *Matsumoto* or *Gupta*, considered alone or in combination, and are therefore patentable over Claims 34-36.

CLAIMS 40-42

Claims 40-42 recite limitations similar to Claims 34-36, except in the context of computer-readable media. It is therefore respectfully submitted that Claims 40-42 are patentable over *Matsumoto* and *Gupta* for at least the reasons set forth herein with respect to Claims 34-36.

CLAIMS 46-48

Claims 46-48 recite limitations similar to Claims 34-36, except in the context of apparatuses. It is therefore respectfully submitted that Claims 46-48 are patentable over *Matsumoto* and *Gupta* for at least the reasons set forth herein with respect to Claims 34-36.

In view of the foregoing, it is respectfully submitted that Claims 18, 19, 23, 24, 28, 29, 34-36, 40-42 and 46-48 each recite one or more limitations that are not taught by *Matsumoto* and *Gupta*, considered alone or in combination, and are therefore patentable over *Matsumoto* and *Gupta*.